CLAIMS

1. A secure processor for a computing device, the processor being operable in a normal mode and a preferred mode, the processor including a security kernel for being instantiated on the processor when the processor enters into the preferred mode and a security key accessible by the instantiated security kernel when the processor is operating in the preferred mode, the security kernel employing the accessed security key during the preferred mode to authenticate a secure application on the computing device, wherein the security kernel allows the processor to be trusted to keep hidden a secret of the application.

2. The processor of claim 1 in combination with the application.

3. The processor of claim 2 wherein the application is selected from a group consisting of a digital rights management (DRM) system and a banking / financial system.

4. The processor of claim 1 wherein the security kernel automatically authenticates a particular application.

5. The processor of claim 1 wherein the security kernel initially authenticates a chooser application that allows a user to select from at least one available applications on the computing device.

6. The processor of claim 1 wherein the security kernel employs the accessed security key during the preferred mode to decrypt at least one encrypted key for the application.

7. The processor of claim 1 in combination with the computing device.

8. The processor of claim 7 wherein the computing device is a portable computing device.

9. The processor of claim 1 further comprising a storage space, the security kernel being permanently stored in the storage space.

10. The processor of claim 1 further comprising a storage space, the security key being permanently stored in the storage space.

11. The processor of claim 1 wherein the security kernel employs the accessed security key during the preferred mode to authenticate / verify the application prior to instantiation thereof.

12. The processor of claim 11 wherein the security kernel performs a hash / MAC (message authentication code) over at least a portion of the application and then compares the hash / MAC to a hash / MAC corresponding to the application.

13. The processor of claim 1 wherein such processor enters preferred mode whenever a predefined initializing processor action is performed.

14. The processor of claim 13 wherein such processor enters preferred mode whenever a CPU reset is performed.

15. A method for a secure processor to instantiate and authenticate a secure application thereon by way of a security kernel, the method comprising:

entering a preferred mode where a security key of the processor is accessible;

instantiating and running a security kernel, the security kernel:

accessing the security key;

applying the accessed security key to decrypt at least one encrypted key for the application;

storing the decrypted key(s) in a location where the application will expect the key(s) to be found; and

authenticating the application on the processor; and

entering a normal mode from the preferred mode after the security kernel authenticates the application, where the security key is not accessible;

wherein the security kernel allows the processor to be trusted to keep hidden the key(s) of the application.

16. The method of claim 15 wherein entering the preferred mode comprises entering the preferred mode upon a CPU reset.

17. The method of claim 15 further comprising erasing data in a cache of the processor prior to instantiating the security kernel.

18. The method of claim 15 further comprising erasing data in a cache of the processor after entering normal mode.

19. The method of claim 15 wherein the security kernel employs the accessed security key during the preferred mode to authenticate / verify the application prior to instantiation thereof.

20. The method of claim 19 wherein the security kernel performs a hash / MAC (message authentication code) over at least a portion of the

application and then compares the hash / MAC to a hash / MAC corresponding to the application.

21. The method of claim 15 wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN; and

applying KMAN to KMAN (KCODE) to produce KCODE.

22. The method of claim 21 wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
MAC (main body, KMAN)	message authentication code of the main body under KMAN
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN;

computing MAC (main body, KMAN);

comparing the computed MAC to MAC (main body, KMAN) from the header to determine if the code image has been changed; and

if the MACs match, applying KMAN to KMAN (KCODE) to produce KCODE.

23. The method of claim 15 wherein the security key of the processor is a private key of a public key - private key pair and the application is instantiated from a code image including a main body and a header including:

public key (KCODE)	KCODE encrypted according to the public key

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises applying the security key as the private key to public key (KCODE) to produce KCODE.

24. The method of claim 23 wherein the security key of the processor is a private key of a public key - private key pair and the application is instantiated from a code image including a main body and a header including:

public key (HASH (main body), KCODE)	Hash of the main body and KCODE, both encrypted according to the public key

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

computing HASH (main body);

applying the private key to public key (HASH (main body), KCODE) to produce HASH (main body) and KCODE;

comparing the computed HASH to the produced HASH to determine if the code image has been changed;; and

if the HASHs match, employing the produced KCODE as appropriate.

25. A method for a secure processor to instantiate one of a plurality of available secure applications thereon by way of a security kernel, the method comprising:

setting a chooser value to a value corresponding to a chooser application upon power-up;

entering a preferred mode upon a power-up CPU reset and instantiating the security kernel, the security kernel determining that the chooser value corresponds to the chooser application and therefore authenticating same, the chooser application being instantiated;

entering a normal mode after the chooser application is instantiated and leaving same to run, the chooser application presenting the plurality of available applications for selection by a user;

receiving a selection of one of the presented applications to be instantiated;

setting the chooser value to a value corresponding to the selected application;

entering a preferred mode upon an executed CPU reset and instantiating the security kernel, the security kernel determining that the chooser value corresponds to the selected application and therefore authenticating same, the selected application being instantiated;

entering a normal mode after the selected application is instantiated and leaving same to run;

wherein the security kernel allows the processor to be trusted to keep hidden a secret of the chooser application and a secret of the selected application.

26. The method of claim 25 further comprising setting the chooser value to the value corresponding to the chooser application upon the selected application being authenticated by the security kernel, wherein upon execution of a CPU reset, the security kernel determines that the chooser value corresponds to the chooser application 72c and therefore authenticates same.

27. The method of claim 25 further comprising storing the chooser value in a memory location not affected by a CPU reset so that the stored chooser value is available after same.

28. A method for a secure processor to instantiate a secure application thereon, the method comprising:

instantiating a first security kernel which employs symmetric cryptography;

instantiating by way of the instantiated first security kernel a second security kernel which employs asymmetric cryptography; and

authenticating by way of the instantiated second security kernel the secure application.

29. The method of claim 28 wherein the security key of the processor is a symmetric key and the second security kernel is instantiated by the first security kernel from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is a security key of the processor, KMAN is a device key independent of the security key, and KCODE is the private key of the second security kernel, and

wherein the first security kernel applies the security key to decrypt the private key of the second security kernel during instantiation thereof by:

applying KCPU to KCPU (KMAN) to produce KMAN; and

applying KMAN to KMAN (KCODE) to produce KCODE.

30. The method of claim 29 wherein the application is instantiated by the second security kernel from a code image including a main body and a header including:

public key (KCODE)	KCODE encrypted according to the public key

where KCODE is the secret of the application, and

wherein the second security kernel applies the private key to decrypt the secret of the application during authentication thereof.

31. A computer-readable medium having stored thereon computer-executable instructions implementing a method for a secure processor to instantiate a secure application thereon by way of a security kernel, the method comprising:

entering a preferred mode where a security key of the processor is accessible;

instantiating and running a security kernel, the security kernel:

accessing the security key;

applying the accessed security key to decrypt at least one encrypted key for the application;

storing the decrypted key(s) in a location where the application will expect the key(s) to be found; and

authenticating the application on the processor; and

entering a normal mode from the preferred mode after the security kernel authenticates the application, where the security key is not accessible;

wherein the security kernel allows the processor to be trusted to keep hidden the key(s) of the application.

32. The medium of claim 31 wherein entering the preferred mode comprises entering the preferred mode upon a CPU reset.

33. The medium of claim 31 wherein the method further comprises erasing data in a cache of the processor prior to instantiating the security kernel.

34. The medium of claim 31 wherein the method further comprises erasing data in a cache of the processor after entering normal mode.

35. The medium of claim 31 wherein the security kernel employs the accessed security key during the preferred mode to authenticate / verify the application prior to instantiation thereof.

36. The medium of claim 35 wherein the security kernel performs a hash / MAC (message authentication code) over at least a portion of the application and then compares the hash / MAC to a hash / MAC corresponding to the application.

37. The medium of claim 31 wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN; and

applying KMAN to KMAN (KCODE) to produce KCODE.

38. The medium of claim 37 wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
MAC (main body, KMAN)	message authentication code of the main body under KMAN
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN;

computing MAC (main body, KMAN);

comparing the computed MAC to MAC (main body, KMAN) from the header to determine if the code image has been changed; and

if the MACs match, applying KMAN to KMAN (KCODE) to produce KCODE.

39. The medium of claim 31 wherein the security key of the processor is a private key of a public key - private key pair and the application is instantiated from a code image including a main body and a header including:

public key (KCODE)	KCODE encrypted according to the public key

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises applying the security key as the private key to public key (KCODE) to produce KCODE.

40. The medium of claim 39 wherein the security key of the processor is a private key of a public key - private key pair and the application is instantiated from a code image including a main body and a header including:

public key (HASH (main body), KCODE)	Hash of the main body and KCODE, both encrypted according to the public key

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

computing HASH (main body);

applying the private key to public key (HASH (main body), KCODE) to produce HASH (main body) and KCODE;

comparing the computed HASH to the produced HASH to determine if the code image has been changed;; and

if the HASHs match, employing the produced KCODE as appropriate.

41. A computer-readable medium having computer-executable instructions thereon implementing a method for a secure processor to instantiate one of a plurality of available secure applications thereon by way of a security kernel, the method comprising:

setting a chooser value to a value corresponding to a chooser application upon power-up;

entering a preferred mode upon a power-up CPU reset and instantiating the security kernel, the security kernel determining that the chooser value corresponds to the chooser application and therefore authenticating same, the chooser application being instantiated;

entering a normal mode after the chooser application is instantiated and leaving same to run, the chooser application presenting the plurality of available applications for selection by a user;

receiving a selection of one of the presented applications to be instantiated;

setting the chooser value to a value corresponding to the selected application;

entering a preferred mode upon an executed CPU reset and instantiating the security kernel, the security kernel determining that the chooser value corresponds to the selected application and therefore authenticating same, the selected application being instantiated;

entering a normal mode after the selected application is instantiated and leaving same to run;

wherein the security kernel allows the processor to be trusted to keep hidden a secret of the chooser application and a secret of the selected application.

42. The medium of claim 41 wherein the method further comprises setting the chooser value to the value corresponding to the chooser application upon the selected application being authenticated by the security kernel, wherein upon execution of a CPU reset, the security kernel determines

that the chooser value corresponds to the chooser application 72c and therefore authenticates same.

43. The medium of claim 41 wherein the method further comprises storing the chooser value in a memory location not affected by a CPU reset so that the stored chooser value is available after same.

44. A computer-readable medium having stored thereon computer-executable instructions implementing a method for a secure processor to instantiate a secure application thereon, the method comprising:

instantiating a first security kernel which employs symmetric cryptography;

instantiating by way of the instantiated first security kernel a second security kernel which employs asymmetric cryptography; and

authenticating by way of the instantiated second security kernel the secure application.

45. The medium of claim 44 wherein the security key of the processor is a symmetric key and the second security kernel is instantiated by the first security kernel from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is a security key of the processor, KMAN is a device key independent of the security key, and KCODE is the private key of the second security kernel, and

wherein the first security kernel applies the security key to decrypt the private key of the second security kernel during instantiation thereof by:

applying KCPU to KCPU (KMAN) to produce KMAN; and

applying KMAN to KMAN (KCODE) to produce KCODE.

46. The medium of claim 45 wherein the application is instantiated by the second security kernel from a code image including a main body and a header including:

public key (KCODE)	KCODE encrypted according to the public key

where KCODE is the secret of the application, and

wherein the second security kernel applies the private key to decrypt the secret of the application during instantiation thereof.